WHAT IS CLAIMED IS:

1. A method for backing up data on a plurality of computers connected via a network, comprising:

forming partnerships between the plurality of computers such that each computer in a partnership commits under agreements to help backup the data of its backup partners;

backing up data in accordance with the agreements; and

periodically verifying that previously backed up data is being retained by the computers committed to act as backup partners in accordance with the agreements.

2. The method of claim 1, further comprising:

selecting potential backup partners from among the plurality computers based on predetermined criteria.

3. The method of claim 1, further comprising:

negotiating the agreements between the plurality of computers based on predetermined requirements, including backup requirements.

4. The method of claim 1, wherein the plurality of computers can administer a distributed cooperative backing up of data in the absence of central control.

5. The method of claim 1, wherein each time before the data is backed up the data is encoded with an erasure code.

6. The method of claim 1, wherein each time before the data is backed up the data is encoded with an error correction code.

7. The method of claim 1, wherein each time before the data is backed up the data is encrypted.

8. The method of claim 1, wherein each time before the data is backed up the data is encoded with an erasure code and then encrypted, the encoding being for fault tolerance and the encryption being for data security.

9. The method of claim 1, wherein each time before the data is backed up the data is compressed and then encoded with an erasure code.

10. The method of claim 9, wherein the compression is a lossless data compression.11.

The method of claim 1, wherein each time before the data is backed up the data is, in sequence, compressed, encoded with an erasure code and encrypted.

1,126

11 ~~12~~. The method of claim 1, wherein each time before the data is backed up the method further comprises, in sequence:

performing data compression;

performing a first data encryption;

performing encoding with an erasure code; and

performing a second data encryption.

12 ~~13~~. The method of claim ~~12~~ 11, wherein the first encryption is for data security and the second encryption is for preventing freeloading by any of the backup partners, and wherein the encoding is for fault tolerance.

13 ~~14~~. The method of claim 1, further comprising:

restoring data from the previously backed up data.

14 ~~15~~. The method of claim 1, wherein each of the plurality of computers has a storage, the storage being periodically scanned to find data to be backed up and identify data previously backed up that no longer needs to be backed up, the data to be backed up being retrieved from the storage for a next periodic backup.

15 ~~16~~. The method of claim 1, wherein verifying that previously backed up data is retained by the backup partners includes monitoring the backup partners, and for any one of the backup partners being monitored,

selecting a block of data stored at the monitored backup partner,

requesting the block of data from the monitored backup partner, and

receiving from the monitored backup partner and checking the block of data to determine if the block of data represents a corresponding block of previously backed up data.

16 ~~17~~. The method of claim 15 ~~16~~, wherein the block is selected randomly.

17 ~~18~~. The method of claim 15 ~~16~~, wherein the block is selected using a protocol to produce a number that corresponds to the selected block.

18 ~~19~~. The method of claim 17 ~~18~~, wherein the protocol, being performed by any computer of the plurality of computers, includes

sending by the computer to a monitored one of its backup partners a hash value of a first random number,

receiving by the computer from the monitored one of its backup partners a second random number,

sending by the computer to the monitored one of its backup partners the first random number,

computing the number from the first and second random numbers by both the computer and the monitored one of its backup partners.

19 ~~20~~. The method of claim 1, further comprising:

selecting another computer connected via the network to be a new backup partner if it is determined that a backup partner has reneged by not retaining the previously backed up data;

negotiating and, if an agreement is reached, forming a partnership with the other computer, accepting the other computer as the new backup partner.

20 20 ~~21~~. The method of claim ~~20~~ 19, wherein selecting another computer to be the new backup partner includes

determining if there are sufficient backup partners for backing up the data, and

searching for the other computer based on predetermined criteria including one or both of geographic separation and system diversity.

21 21 ~~22~~. The method of ~~20~~ 19, wherein if after accepting the other computer as the new backup partner it is determined that the backup partners are insufficient in number for backing up the data, the selecting, negotiating and forming backup partnership with yet another computer are repeated, the determining, selecting, negotiating and forming backup partnership being repeated until the number of backup partners is sufficient.

22 22 ~~23~~. The method of claim 2, wherein selecting computers as potential backup partners includes

determining if there are sufficient backup partners for backing up the data, and

searching for computers based on the predetermined criteria that includes one or both of geographic separation and system diversity.

23 23 ~~24~~. The method of claim 3, wherein negotiating the agreements includes, for any computer of the plurality of computers,

exchanging queries between the computer and computers selected as its potential backup partners about each such computer's ability to satisfy the predetermined requirements that include one or more of

predictable and suitable time schedule for being on-line,

suitable network bandwidth,

matching backup space requirements, and

backup track record.

24 24 ~~25~~. The method of claim ~~24~~ 23, wherein, the computer prefers to partner with those of its potential backup partners that satisfy the predetermined requirements.

25 25 ~~26~~. The method of claim 23 ~~24~~, wherein the suitable network bandwidth is equal or larger than a predetermined threshold bandwidth and is characterized by an average bandwidth that is larger than the predetermined threshold bandwidth.

26 26 ~~27~~. The method of claim 23 ~~24~~, wherein the backup track record includes not reneging on a number of other backup partners that is greater than a predetermined number.

27 27 ~~28~~. The method of claim 1, wherein each of the backup partners has a recent copy of a list of its backup partners' other backup partners.

28 28 ~~29~~. The method of claim 1, wherein a user of each of the plurality of computers can obtain a copy of a list containing identifiers and/or identities of the backup partners associated therewith and an encryption key under which the data is encrypted prior to being backed up.

29 29 ~~30~~. The method of claim 1, wherein the agreements are respectively negotiated between the plurality of computers such that in each partnership each computer commits to avoid making or honoring data restoration requests for a predetermined commitment period that is longer than a grace period, wherein the grace period for a backup partner of a computer starts to run if it is determined that the backup partner has failed to respond to such computer verifying that the backup partner is retaining the previously backed up data or to prove to such computer that it is retaining the previously backed up data, and wherein upon the grace period running out such computer considers the backup partner to have reneged on its agreement.

30 30 ~~31~~. The method of claim 7, wherein any encryption algorithm can be suitably used for encrypting the data being backed up, including DES (data encryption standard), RC4, RSA or other public-key encryption.

31 31 ~~32~~. The method of claim 6, wherein the error correction code is a Reed Solomon code.

32 ~~33~~.32 The method of claim 5, wherein for a low degree of fault tolerance the erasure code is *n+1-parity*.

33 33 ~~34.~~ The method of claim 7, wherein after the encryption of the data the encrypted data is divided into blocks and cryptographic checksums or digital signature are added to each block before the blocks are sent each to a particular one of the backup partners.

34 34 ~~35.~~ The method of claim 5, wherein the encoding with the erasure code uses Tornado coding.

35 35 ~~36.~~ The method of claim 5, wherein the encoding with the erasure code includes

dividing the data being backed up into blocks, and

adding redundancy to each of the blocks producing data objects with actual data portions and redundant data portions, so that each one of the actual data portions and redundant data portions is being backed up at a distinct one of the backup partners.

36 36 ~~37.~~ The method of claim 1, further comprising:

dividing the data being backed up into blocks;

creating a hash value of each of the blocks using a key; and

correspondingly appending the hash values to their blocks before the blocks are each sent to a distinct one of the backup partners.

37 37 ~~38.~~ The method of claim ~~37~~ 36, wherein the hash values are later used in periodically verifying that the previously backed up data is retained by the backup partners and, if needed, that the previously backed up data being retained is valid and can be used to restore lost data.

38 38 ~~39.~~ The method of claim ~~37~~ 36, wherein the periodic verifying includes

selecting and requesting a particular one of the data blocks that was previously backed up,

retrieving the particular one of the data blocks and its associated hash value,

computing a new hash value from the retrieved particular block using the key, and

comparing the new hash value with the associated hash value to determine it they are equal, equality indicating that the data block is retained by the backup partner and is valid.

39 ~~40.~~ 39 The method of claim 1, wherein the encoding includes

dividing the data being backed up into *p* groups of *m* blocks, each of the *p* groups representing a vector of actual data and the *m* blocks in each of the *p* groups representing *m* elements of the actual data vector; and

adding redundancy to each actual data vectors producing *p* codewords each being a vector of *n=m+k* elements, so that each one of the *n* elements is being backed up at a distinct one of the backup partners.

40 ~~41.~~ 40 The method of claim ~~14~~ 13, wherein the restoring of data from the previously backed up data includes

retrieving blocks of the previously backed up data from the backup partners until sufficient blocks of the previously backed up data are available for decoding,

checking, for each retrieved block of the previously backed up data, if the retrieved block is valid and intact,

decoding all the retrieved blocks of the previously backed up data to reconstruct the data originally backed up.

41 ~~42.~~ 41 The method of claim ~~14~~ 13, wherein the restoring of data from the previously backed up data includes

retrieving previously backed up data from the backup partners until sufficient previously backed up data is available for decoding,

decoding all the retrieved previously backed up data to reconstruct the data originally backed up, and

decrypting the data originally backed up to obtain the actual data.

42 ~~43.~~ 42 The method of claim ~~14~~ 13, wherein the restoring of data from the previously backed up data includes

retrieving previously backed up data from the backup partners until sufficient previously backed up data is available for decoding, and

decrypting, decoding and decompressing all of the retrieved previously backed up data.

43 43 ~~44~~. The method of claim 1, wherein the data being backed up is file contents.

44 44 ~~45~~. A distributed cooperative backup system, comprising:

a network; and

a loose confederation of computers connected via the network, a plurality of computers from among the loose confederation of computers being configured for distributed cooperative backing up of data, each computer of the plurality of computers having a storage that can be used for providing reciprocal backup services, and each computer of the plurality of computers respectively having a computer readable medium embodying computer program code configured to cause the computer to

form partnerships between the plurality of computers, each of the partnerships being of computers such that each computer in a partnership commits under agreements to help backup the data of its backup partners;

back up data in accordance with the agreements; and

periodically verify that previously backed up data is being retained by the computers committed to act as backup partners in accordance with the agreements.

45 45 ~~46~~. The system of claim 44 ~~45~~, wherein each of the backup partners may leave the system and return to the system at any time.

46 46 ~~47~~. The system of claim 44 ~~45~~, wherein prevention of freeloading is enforced by the backup partners themselves, wherein any one of the backup partners may be periodically requested to prove that it is retaining the previously backed up data.

47 47 ~~48~~. A distributed cooperative backup system, comprising:

a network; and

a loose confederation of computers connected via the network, a plurality of computers from among the loose confederation of computers being configured for distributed cooperative backing up of data and functioning as backup partners, each computer of the plurality of computers having a storage that can be used for providing reciprocal backup services, and each computer of the plurality of computers respectively having a computer readable medium embodying computer program code configured to cause the computer to

select computers as potential backup partners from among the plurality of computers based on predetermined criteria,

negotiate a reciprocal backup partnership agreement between the computer and selected computers based on predetermined requirements, including backup requirements,

form partnerships between the computer and the selected computers, the computer and the selected computers becoming backup partners by agreeing to cooperatively provide backup services to each other so that a distributed cooperative backing up of data can be administered in the absence of central control,

periodically back up data at the backup partners, encoding the data each time before the data is backed up, and

periodically verify that previously backed up data is retained by the backup partners.